DEFENSE IN DEPTH

Squashing the Worm

Barbara Chung
Sr. Technology Specialist
National Technology Team
Microsoft Corporation

Agenda

- The Problem(s)
- Some Solutions

The Big Problem

- Time between discovery of vulnerability and exploit has diminished to a very small window of time
  - Not much time (or none) to test patches before deployment
  - Given how we do business today, it's hard to catch all clients before they are infected

Slammer: A Good Example of a Bad Thing

- Attack on MS SQL Server, UDP/1434
  - Patch previously available
  - Good patching operations for servers in place
  - Rare to find SQL directly exposed to Internet
  - Easy to block UDP/1434 at the firewall

  Sounds like a no-brainer, right?

Slammer: Why was it so serious?

- Also attacked MSDE on the client, UDP/1434
  - MSDE installed by user apps front-ending it, most customers not sure where it was installed and how many instances
  - Client machines all over the place
- Customers locked down firewalls—those who didn't weren't patched were nailed by infected clients coming in over VPN

Lessons Learned To Date

- You *must* manage both servers and clients
- You *must* have testing/patching operations in place
- You should know how to protect clients until they can be patched
  - Block the attack on the client if possible
- Protect all points of access
  - Authenticate all machines *before* they get to your network to prevent rogue machines from entering
- Regularly monitor machines for security state, including those coming in over VPN/dial-up

Managing Clients for Security

- **Baseline Your Clients for a Secure Configuration**
  - **Windows 2000 Baseline Security Checklist**
    http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2kprocl.asp
  - **Windows XP Baseline Security Checklists**
    http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/xpcl.asp

Managing Clients for Security

- Regularly scan for
  - The correct service pack or the latest security patches installed
  - The correct antivirus software and signature files installed
  - Firewall software installed and active on the Internet interface (be sure you can automatically disable this on the LAN)
  - A password-protected screensaver with an adequate wait time
  - Routing disabled (remote access clients)

Patching Options

Feature Area	Windows Update	SUS 1.0 SP1	SMS with SUS Feature Pack
Centralized administration	**Poor.** Computers install updates selected by user.	**Good.** Updates approved by administrator.	**Best.** Updates approved by administrator and specifically targeted.
Central inventory	**Poor.** No central inventory or assessment.	**Poor.** No central inventory or assessment.	**Best.** Customizable central inventory for hardware, software, and vulnerabilities.
Software coverage	**Good.** All types of Windows updates. Windows only.	**Fair*.** Security patches, critical updates, updates, and update rollups. Windows only.	**Best.** Distributes any software or software updates to SMS clients.
Cost	**Free.**	**Free.**	**License fees required.**
Windows operating systems	**Good.** Windows 98, Windows 98 SE, Windows Millennium Edition, Windows XP, Windows 2000, and Windows 2003.	**Fair.** Windows XP, Windows 2000, and Windows 2003.	**Best.** Windows 95, Windows 98, Windows 98 SE, Windows Millennium Edition, Windows NT® 4.0, Windows XP, Windows 2000, and Windows 2003.
Reporting	**Poor.** No central reporting.	**Fair.** Some central reporting through log files.	**Best.** Built-in Web reports and customizable reports.
Architecture and install	**Easy.** Client configuration only; no other infrastructure.	**Easy.** Simple server architecture: easy client setup.	**Hard.** Complex architecture and services installation.

* SUS 1.0 SP1 may include service packs in the near future; turning this from Fair to Good.

Block the Attack on the Client (Interim Protection)

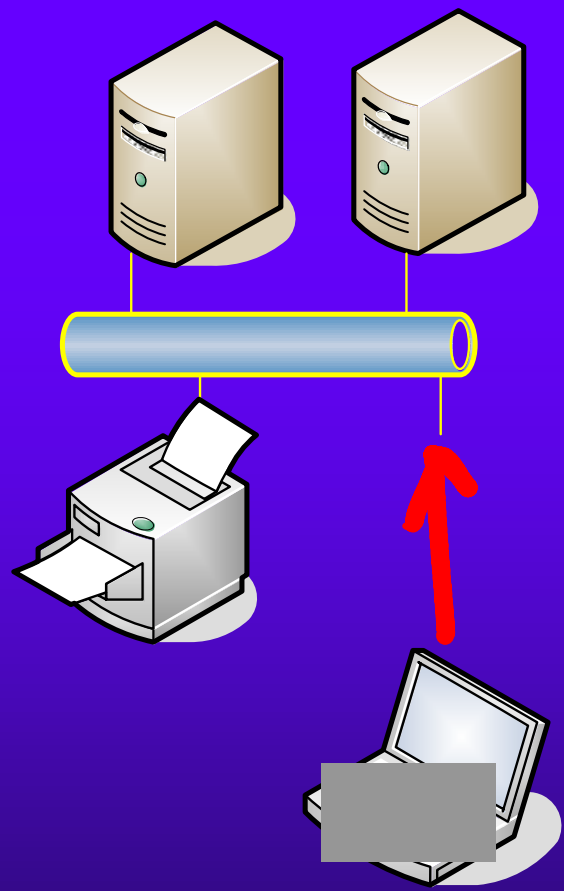
- IPSec
  - Wire protocol for securing communications
  - You can require authenticated/encrypted connection
  - You can BLOCK ports/protocols (used to protect against Slammer and later RPC worms)
  - Built into Windows 2000, Windows XP, Windows Server 2003, managed via command-line, script or Active Directory group policy
  - Very powerful…you'll need to understand implications of blocking well in advance, particularly if IPSec policy is already deployed

Authenticating Machines Before They Join the Network

- 802.1x on Wired Networks
  - Authentication protocol works with smart network devices to determine if client should be allowed on the network
  - Prevents rogue machines from accessing the network
  - Can use certificates or integrated-Windows authentication
  - In addition, when used with VLAN, machines can be restricted to particular areas of the network based on group membership of either machine or user

Wired Networks

- A visitor/attacker attaches to an open network tap. He gets an IP address. If he is infected with a worm and your machines aren't patched—you're probably toasted.
- If he has deliberate malicious intent, he can poke around the network for goodies.

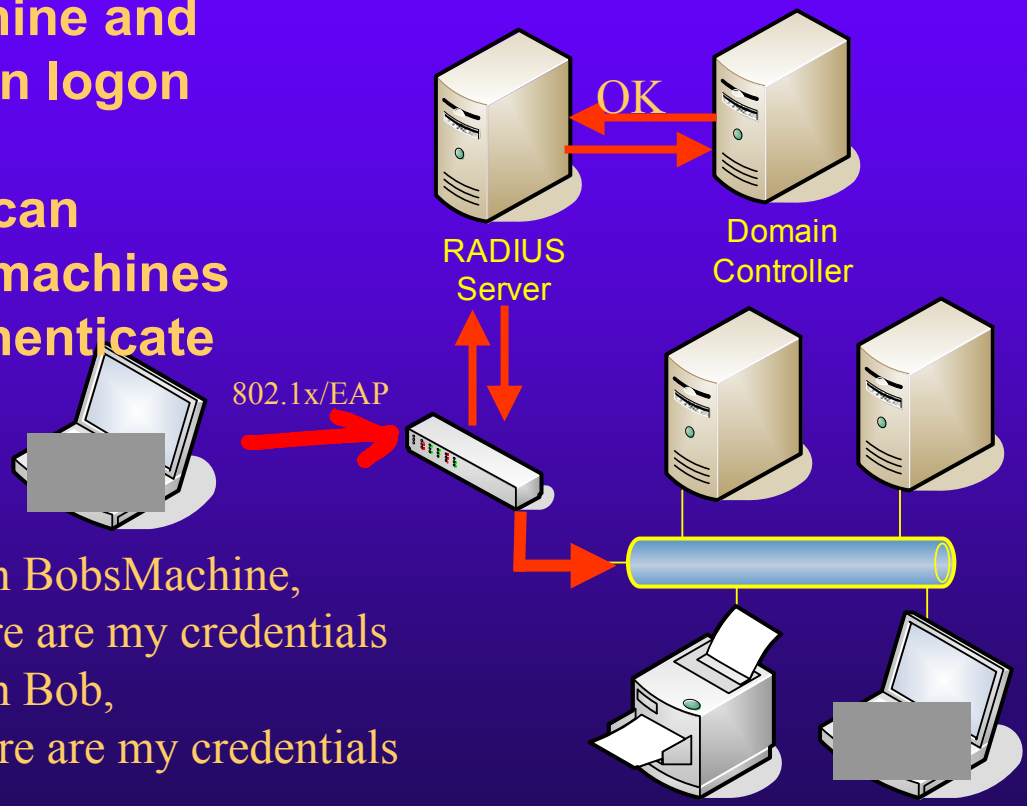


802.1x on Wired Networks: Components

- Active Directory domain
- RADIUS Server (actually 2 of them for redundancy) with certificates installed
- Wired remote access policy
- Multiple authentication switches (must support 802.1x and RADIUS)
- Certificate Services if using certs for authentication
- Works with Windows XP, Windows 2000, downlevel clients (Windows 95, Windows 98, Windows NT 4.0 for customers with Premier support)

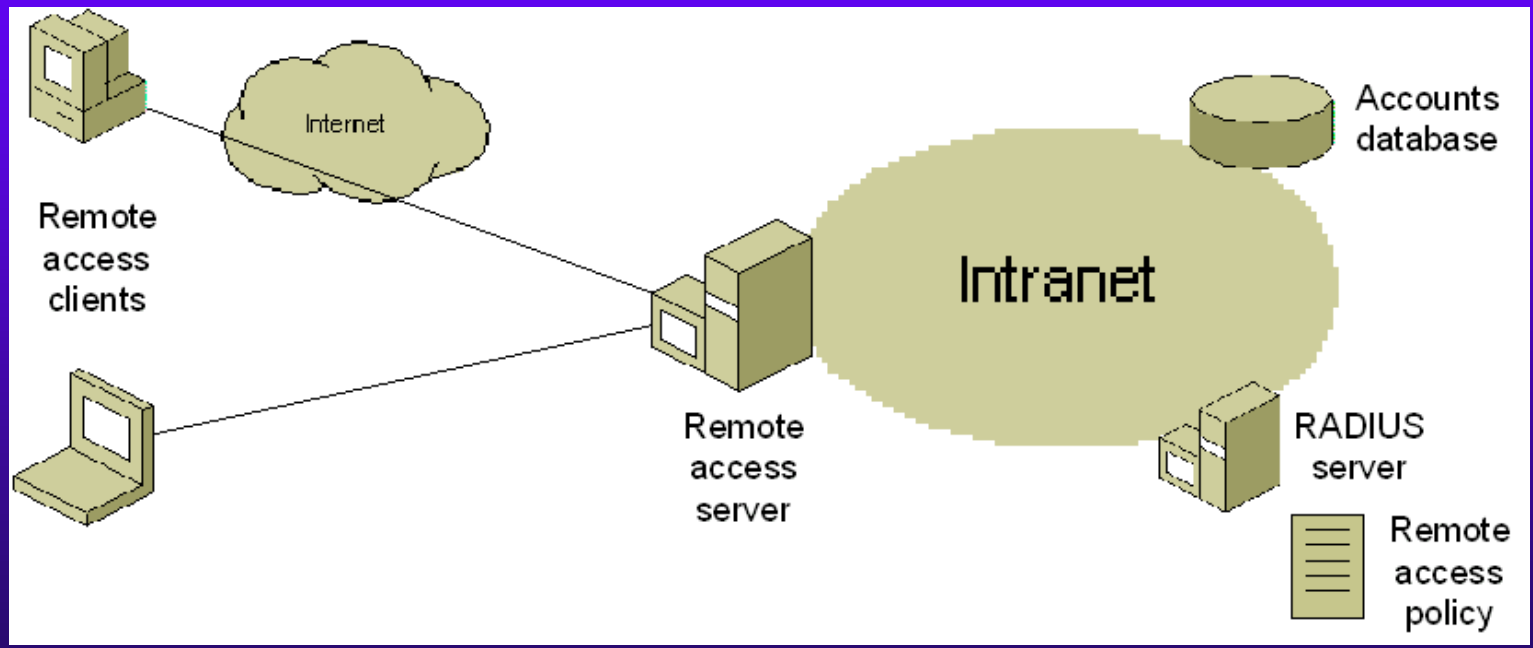
802.1x on Wired Networks

- **Client connects and is sandboxed until his credentials are verified**
- **Use both machine and user auth, to run logon scripts**
- **Guest access can accommodate machines that do not authenticate**



Incoming VPN Clients

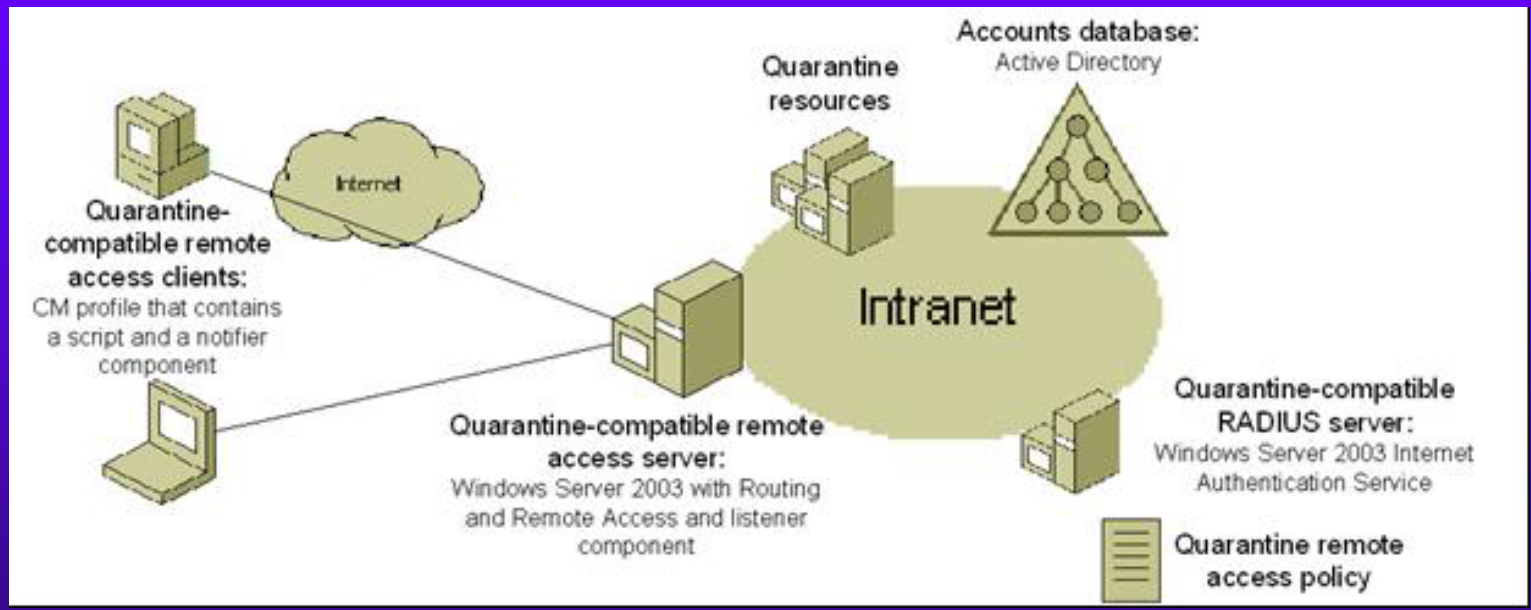
Your user/machine is legit, but his machine may be carrying a worm



Scanning VPN Clients

- Network Access Quarantine Control
  - New in Windows Server 2003
  - Delays normal remote access to a private network until the configuration of the remote access computer has been examined and validated by an administrator-provided script.

Scanning Incoming VPN Clients for Security State



Questions?

Where do you want to go today?®

Microsoft®